Sommario

Sei solo a una password debole da una violazione...
.... E anche le tue password "complicate" possono essere violate.

Le password semplicemente non sono più sufficienti per proteggere le tue risorse, i tuoi account e le tue informazioni.
Ecco alcune prove del perché:

L'80% degli utenti RIUTILIZZA

password tra account2

Il 6% degli utenti di Internet utilizza il

STESSA password su tutti gli account online2

Circa il 46% dei dipendenti

utilizzare **password personali**
per gli account aziendali3

Le persone scelgono password deboli

Le prime 25 password deboli nel 20171

1. 123456
2. Parola d'ordine
3. 12345678
4. qwerty
5. 12345
6. 123456789
7. più tardi
8. 1234567
9. calcio
10. ti amo
11. admin
12. benvenuto
13. scimmia
14. login
15. abc123
16. guerre stellari
17. 123123
18. drago
19. passw0rd
20. master
21. ciao
22. libertà
23. qualunque cosa
24. qazwsx
25. trustno1

1. https://www.teamsid.com/worst-passwords-2017-full-list/
2. https://www.csoonline.com/article/3244137/password-security/password-managers-grow-up-target-business-users.html
3. http://www.statista.com/statistics/763091/us-use-of-same-online-passwords
4. https://www.fastcompany.com/40469838/dashlane-reused-password-hygiene

Pensi che le tue password siano forti? Questo non fermerà gli hacker.

Possono semplicemente **acquistare le credenziali sul dark web** in modo simile a come faresti un acquisto su amazon.com.

Prezzo medio di una password sul dark web5 : **$ 160,15**

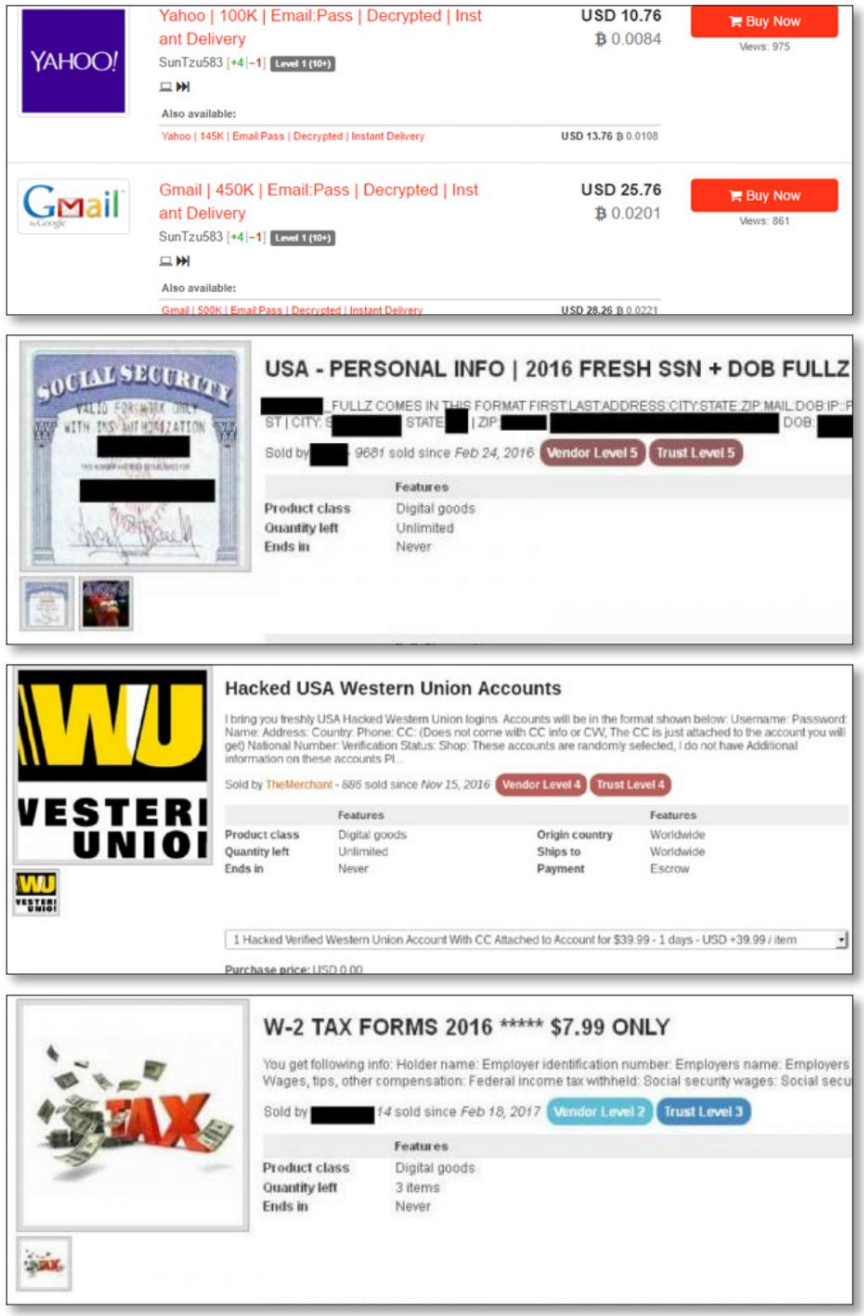
Valore medio dell'identità di un utente (credenziali tra gli account) per un hacker: **$ 1.200.**

Se il tuo IP, informazioni finanziarie, informazioni sui clienti, informazioni sui dipendenti o qualsiasi altra cosa nella tua rete vale più di $ 1.200, è semplice economia che sia redditizio per un hacker acquistare l'accesso (cioè le tue credenziali) a tali informazioni.

Pensi che non accadrebbe alle tue credenziali? O le credenziali del tuo collega?

Sul dark web sono disponibili miliardi di credenziali, molte delle quali appartengono agli utenti amministratori. Solo alla fine del 2017 è stato scoperto un singolo file contenente 1,4 miliardi di password in testo semplice.6 È probabile che le tue informazioni di accesso possano essere acquistate in pochi secondi.

Una volta sul dark web, acquistare le tue password è facile come fare un acquisto su Amazon. A destra ci sono alcune immagini di pagine di acquisto di credenziali del dark web.



5. https://www.nbcnews.com/tech/security/your-identity-sale-dark-web-less-1-200-n855366
6. https://medium.com/4iqdelvedeep/1-4-billion-clear-text-credentials-discovered-in-a-single-database-3131d0a1ae14
7. http://www.cyberinject.com/gmail-yahoo-passwords-on-dark-web/
8. https://www.theteneogroup.com/2017/06/08/understanding-deep-web-dark-web-guard-network/
9. https://zerohedge.whotrades.com/blog/43790836676
10. https://zerohedge.whotrades.com/blog/43790836676

Se un hacker sceglie di decifrare la tua password invece di acquistarla, **probabilmente non impiegherà molto a farlo.**

In effetti, potrebbero decifrare le password della maggior parte delle persone nel tempo necessario per leggere questa tabella11

Tipo	Parola d'ordine	Tempo (HSIMP) Quanto è sicura la mia password?	Tempo (PA) Fallimento Strumento di analisi	Sicurezza Livello
Parola comune di 8 caratteri obbligatoria		52 secondi	<1 giorno	Inutile
8 caratteri casuali	qkcrmztd	52 secondi	<1 giorno	Inutile
8 caratteri casuali con numeri	kqwbv832	11 minuti	<1 giorno	Inutile
8 caratteri casuali con maiuscole, simboli e numeri misti	J5bZ>9p!	20 giorni	<1 giorno	Rischioso

Tipo	Parola d'ordine	Tempo (HSIMP)	Tempo (PAPÀ)	Sicurezza Livello
Password di 2 parole comuni	tè all'arancia	98 giorni	<1 giorno	Rischioso
Password di 3 parole comuni	questo è bello	546 anni	<1 giorno	Rischioso
Password di 5 parole non comuni	du-bi-du-bi-doo	12 milioni di anni	<1 giorno	Rischioso

Le password sono facili da hackerare e forniscono solo una riga di difesa. Se un hacker può rubare solo la password di un dipendente, di solito possono accedere all'intera rete. Una volta dentro, possono fare quello che vogliono. Questo di solito significa diffondere malware o rubare, modificare o eliminare informazioni critiche.

11. https://crambler.com/password-security-why-secure-passwords-need-length-over-complexity/

Ecco una panoramica semplificata che mostra come un hacker ruba la tua password,

come descritto in "Hacking the Hacker" dall'esperto di sicurezza informatica e cappello bianco Roger Grimes:

Raccogliere Informazione
(Fingerprinting e/o ingegneria sociale)

Accedi al tuo Account
probabilmente utilizzando le tue credenziali perse o rubate

Mossa Attorno a Sistema
alle vulnerabilità dell'identità

Ottieni amministrazione Accesso
(Aumento dei privilegi)

Eseguire attacco

Secondo Grimes: ***"Se l'hacker ha fatto i compiti nella fase di rilevamento delle impronte digitali, allora questa fase non è affatto difficile".***

Vale a dire, è facile per gli hacker accedere ai tuoi account. Alcuni coprono anche le loro tracce o creano una porta per l'accesso futuro, anche se non è sempre così.

Rubare la tua password è facile

Il processo di furto di una password è incredibilmente facile (e redditizio) per gli hacker. I loro strumenti e tecnologie per indovinare la password sono diventati esponenzialmente più sofisticati e automatizzati al punto che spesso non è necessario "indovinare" manualmente la password. Anche quando lo è, algoritmi avanzati, ingegneria sociale (ad es. attacchi di phishing o cavalli di Troia), keylogging e altri metodi consentono loro di indovinare e testare in modo efficiente le password più probabili, il che molto spesso ha successo.

Alcuni metodi comuni di hacking delle password includono:

Dizionario Attacco

Gli hacker cercano di indovinare una password digitando un comune elenco di parole da un "dizionario" di password. I dizionari di password più avanzati includono elenchi delle parole più comunemente utilizzate nelle password. Questo è un metodo relativamente semplice, ma efficace per indovinare password meno complesse. Se usi parole reali in una qualsiasi delle tue password, le tue credenziali sono a rischio.

Attacco di forza bruta

Sebbene non sia efficiente come un attacco con dizionario, un attacco di forza bruta è più efficace nell'indovinare una password. Con questo metodo, gli hacker utilizzano strumenti per provare ripetutamente ogni possibile combinazione di password di lettere, numeri e simboli finché la password non viene violata.
Un approccio simile è un attacco di forza bruta inversa, in cui un hacker prova una password contro molti nomi utente.

Attacco Arcobaleno

Questo metodo utilizza una risorsa chiamata tabella arcobaleno per decifrare gli hash delle password (essenzialmente password criptate archiviate nei database di sistema) in un modo molto più efficiente ed efficace rispetto agli attacchi di forza bruta o dizionario.

Attacco di riempimento delle credenziali

Poiché così tante persone utilizzano le stesse password o variazioni di password tra gli account, gli hacker hanno trovato un modo per eseguire automaticamente elenchi di database di combinazioni di nome utente/password violate contro l'accesso a un sito Web di destinazione. Secondo Shape Security, Il 90% dei tentativi di accesso ai rivenditori online proviene da questo tipo di attacco e questo metodo è efficace per gli hacker circa il 3% delle volte.

Ingegneria sociale

Questo approccio si presenta in una serie di stili, tutti radicati nell'idea di ingannare o manipolare le persone affinché divulghino le loro informazioni o intraprendano una determinata azione. I comuni metodi di ingegneria sociale utilizzati per rubare le password includono il phishing e l'utilizzo di un attacco di cavalli di Troia. Un approccio meno comune è lo shoulder surfing, in cui l'hacker osserva semplicemente un utente che digita la propria password.

Con la crescente sofisticazione delle tecnologie e degli strumenti degli hacker, il passaggio più semplice di un hack è spesso quello di decifrare la password. In effetti, è così facile che molte volte non richiede nemmeno di indovinare. La parte più spaventosa di questo è che, indipendentemente da quanto sia sicura la tua password, tutto ciò che serve è la password debole di un collega per mettere l'intero sistema della tua azienda a rischio di violazione.

Difesa dell'autenticazione:

Cambiare il comportamento dei dipendenti riguardo alle password semplicemente non funziona

Un metodo per mitigare il rischio di furto di una password consiste nell'addestrare i dipendenti a creare password più sicure ea modificarle più frequentemente. Tuttavia, cambiare il comportamento di ogni singolo dipendente non è solo impegnativo, ma in questo caso inefficace.

Storicamente, questo approccio non funziona

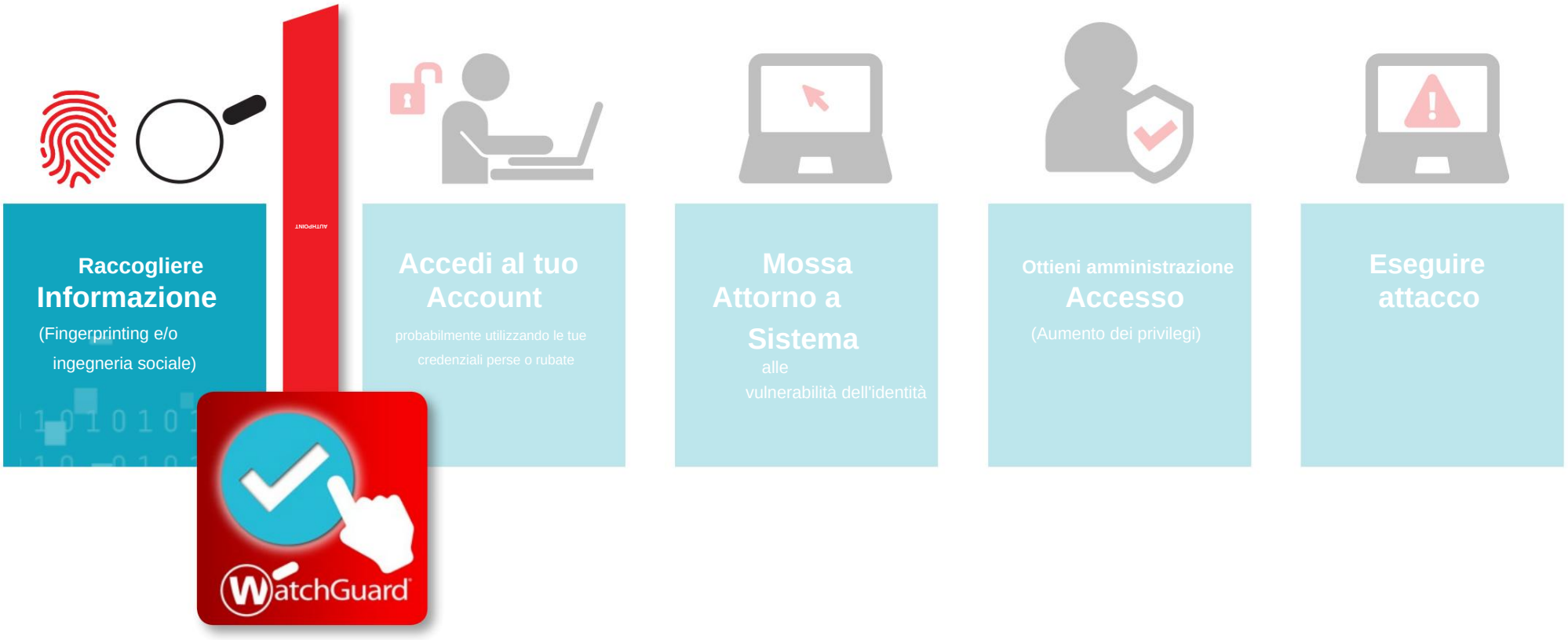
Ciò è dimostrato dai milioni di aziende i cui database sono stati violati e dalle decine di milioni di password trapelate disponibili online (si noti che è possibile acquistare molte di queste credenziali sul dark web).

Crea un'esperienza utente eccessivamente complessa

L'utilizzo di password univoche, completamente randomizzate e di 16 caratteri tra gli account è complesso. Il motivo per cui le persone usano password semplici è che le password sono difficili da ricordare. Molte persone ne creano di leggermente più complesse, ma compensano tale complessità riutilizzando la stessa password (o varianti di essa) tra gli account.

Dal momento che le password non sono sufficienti, che cos'è?

L'autenticazione a più fattori (MFA) è un metodo di verifica che aggiunge un livello di sicurezza agli accessi oltre a un semplice nome utente e password. Aiuta a garantire che gli hacker non possano accedere ai tuoi sistemi anche se una delle password dei tuoi dipendenti viene compromessa.



WatchGuard offre una soluzione di autenticazione a più fattori facile da usare che aiuta le aziende mantengono al sicuro le proprie risorse, informazioni e identità degli utenti: AuthPoint.

AuthPoint® è facile da implementare, facile da gestire ed è disponibile a meno del costo di una tazzina di caffè al mese per utente. È anche più sicuro dell'autenticazione a due fattori (2FA), più sicuro delle soluzioni basate su SMS, più economico (TCO inferiore) rispetto alle soluzioni non basate su cloud e più facile per gli utenti finali rispetto alle soluzioni che richiedono token.

Nota di cautela:
Non tutte le soluzioni MFA sono uguali

L'autenticazione a più fattori basata su SMS non è più un metodo affidabile e sicuro. Gli utenti con autenticazione basata su SMS devono migrare immediatamente ad altri metodi. Nelle sue linee guida sull'identità digitale del 2016, il National Institute of Standards and Technology (NIST) ha incoraggiato gli utenti ad abbandonare l'autenticazione basata su SMS:

"A causa del rischio che i messaggi SMS possano essere intercettati o reindirizzati, gli implementatori di nuovi sistemi dovrebbero considerare attentamente autenticatori alternativi. Autenticazione fuori banda l'uso di [SMS o voce] è deprecato e si sta prendendo in considerazione la rimozione nelle future edizioni di questa linea guida.

L'Harvard Business Review è andato anche oltre, affermando: "si potrebbe sostenere che l'autenticazione tramite SMS sia diventata più un vettore di attacco che una misura di sicurezza".

Il motivo per cui l'autenticazione basata su SMS è rischiosa è che i messaggi di testo sono vulnerabili all'intercettazione. Reddit ne è stata una vittima notevole nel 2018. Reddit ha commentato l'attacco sul proprio sito, attribuendo l'attacco alla debolezza dell'autenticazione basata su SMS: "Abbiamo appreso che l'autenticazione basata su SMS non è così sicura come speravamo e l'attacco principale è avvenuto tramite l'intercettazione di SMS. Lo segnaliamo per incoraggiare tutti qui a passare alla 2FA basata su token".

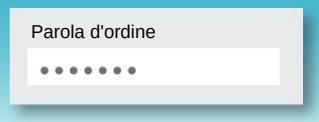
Sebbene l'utilizzo dell'autenticazione MFA basata su SMS sia migliore rispetto a fare affidamento solo su una password e un nome utente, lascia comunque gli utenti vulnerabili agli attacchi di hacker. Per mitigare questo rischio, le aziende dovrebbero fare affidamento su MFA che utilizza solo metodi di autenticazione più forti.

Come funziona AuthPoint?

AuthPoint è un servizio di autenticazione a più fattori (MFA) che aiuta le aziende a proteggere le proprie risorse, informazioni e identità degli utenti. Funziona richiedendo agli utenti di utilizzare 2+ fattori di autenticazione per accedere, piuttosto che fare affidamento solo su una password.

Questi fattori sono una combinazione di:

- **Qualcosa che conosci** (password, PIN)
- **Qualcosa che hai** (gettone, cellulare)
- **Qualcosa che sei** (impronta digitale, volto)

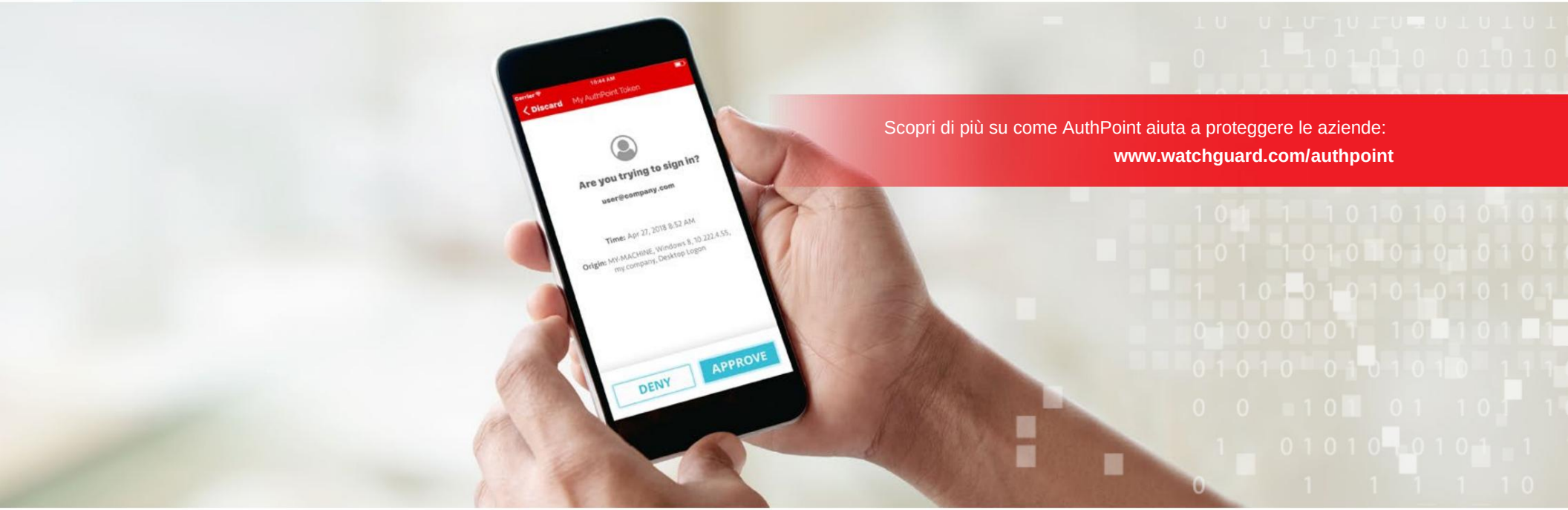


Utilizzando **più livelli di autenticazione,** le aziende possono ridurre significativamente il rischio che i propri account vengano violati. Se un hacker ottiene la password di un dipendente, c'è ancora un altro livello di sicurezza per aiutare a prevenire l'hack.

Con AuthPoint, questa protezione è semplice. Gli utenti approvano o rifiutano gli accessi con un solo tocco sull'app mobile AuthPoint. Una volta effettuato l'accesso, gli utenti possono usufruire del Single Sign-On (SSO) tra gli account chiave.

Poiché le approvazioni vengono tutte effettuate tramite l'app mobile dell'utente, non ci sono token aggiuntivi da trasportare. È facile! AuthPoint si basa interamente sul cloud. Ciò significa che non c'è hardware costoso da implementare e nessun software da aggiornare. Può anche essere gestito da qualsiasi luogo e, poiché è così facile da implementare e gestire, non richiede un esperto di sicurezza interno per iniziare.

Viaggi per lavoro? AuthPoint funziona sia online che offline, il che significa che gli utenti possono accedere in modo sicuro anche se accedono al proprio account da un aereo. Utilizzando l'autenticazione basata su codice QR, gli utenti possono accedere ovunque e in qualsiasi momento.



Scopri di più su come AuthPoint aiuta a proteggere le aziende:
www.watchguard.com/authpoint

AuthPoint fa per te?

Poiché le password vengono facilmente rubate o violate, molte organizzazioni stanno adottando l'autenticazione a più fattori come mezzo per proteggere le identità e le risorse degli utenti. WatchGuard vuole fare questo protezione disponibile per aziende di tutti i tipi e dimensioni, quindi ha creato l'autenticazione a più fattori AuthPoint. L'autenticazione a più fattori lo è una delle protezioni più importanti necessarie per proteggere le piccole e medie imprese moderne ed è ora disponibile tramite il tuo rivenditore WatchGuard.

Una potente protezione è a tua disposizione a meno del prezzo del tuo cappuccino mattutino.

Quindi, scommetteresti la tua attività sulla forza della password di ogni dipendente?
Con AuthPoint, non è necessario. È conveniente, è potente ed è facile da usare.

Contatta il tuo rivenditore WatchGuard per iniziare oggi la tua prova gratuita di 1 mese di AuthPoint.
Per ulteriori informazioni su AuthPoint, visitare www.watchguard.com/authpoint.

IL PORTAFOGLIO DI SICUREZZA DI WATCHGUARD

Sicurezza della rete

Oltre a fornire sicurezza di livello aziendale, la nostra piattaforma è progettata da zero per concentrarsi sulla facilità di implementazione, utilizzo e gestione continua, rendendo WatchGuard la soluzione ideale per le PMI, le medie imprese e le organizzazioni aziendali distribuite in tutto il mondo.

Wi-Fi sicuro

La soluzione Secure Wi-Fi di WatchGuard, un vero punto di svolta nel mercato odierno, è progettata per fornire uno spazio aereo sicuro e protetto per gli ambienti Wi-Fi, eliminando al contempo i grattacapi amministrativi e riducendo notevolmente i costi. Con ampi strumenti di coinvolgimento e visibilità nell'analisi aziendale, offre il vantaggio competitivo di cui le aziende hanno bisogno per avere successo.

Autenticazione a più fattori

WatchGuard AuthPoint® è la soluzione giusta per colmare il divario di sicurezza basato su password che rende le aziende vulnerabili a una violazione. Fornisce l'autenticazione a più fattori su una piattaforma cloud di facile utilizzo. Il nostro approccio unico aggiunge il "DNA del telefono cellulare" come fattore identificativo per garantire che solo l'individuo corretto abbia accesso alle reti sensibili e alle applicazioni cloud.

Scopri di più

Per ulteriori dettagli, parla con il tuo rivenditore WatchGuard autorizzato o visita **https://www.watchguard.com.**

Informazioni su WatchGuard

WatchGuard® Technologies, Inc. è un leader globale nella sicurezza di rete, Wi-Fi sicuro, autenticazione a più fattori e intelligence di rete. I pluripremiati prodotti e servizi dell'azienda godono della fiducia di quasi 10.000 rivenditori e fornitori di servizi di sicurezza in tutto il mondo per proteggere più di 80.000 clienti. La missione di WatchGuard è rendere la sicurezza di livello aziendale accessibile alle aziende di ogni tipo e dimensione attraverso la semplicità, rendendo WatchGuard una soluzione ideale per aziende distribuite e PMI. La società ha sede a Seattle, Washington, con uffici in Nord America, Europa, Pacifico e America Latina. Per saperne di più, visita WatchGuard.com.

Vendite in Nord America: 1.800.734.9905 • Vendite internazionali: 1.206.613.0895 • Web: www.watchguard.com/authpoint

N. parte WGCE67135_022019